

U.S. DISTRICT COURT
N.D. OF N.Y.
FILED
MAR 31 2017

UNITED STATES DISTRICT COURT
for the
Northern District of New York

LAWRENCE K. BAERMAN, CLERK
ALBANY

Case No. **1:17-mj-131-DJS**

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
Information associated with Dropbox accounts)
corresponding to the email addresses)
doetrustin2@mail.com,
lawrencebishop13@yahoo.com, and
tristinjames6969@gmail.com that are stored at
premises controlled by Dropbox, Inc., located in
the Northern District of California

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:
(identify the person or describe the property to be searched and its given location):

See Attachment A

located in the Northern District of California, there is now concealed
(identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 2252A(a)(2)	Receiving and Distributing Child Pornography

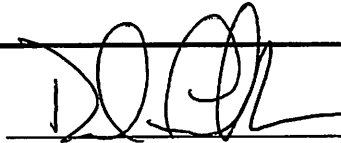
The application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.
 - ☐ Delayed notice of _____ days (give exact ending date if more than 30 days): Click here to enter a date.
- is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

1:17-mj-00131-DJS

AO 106 (Rev. 04/10) Application for a Search Warrant (Page 2)



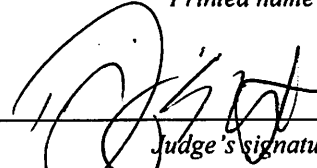
Applicant's signature

Dave Fallon, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: March 31, 2017



Judge's signature

City and State: Albany, NY

Hon. Daniel J. Stewart, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK**

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
DROPBOX ACCOUNTS CORRESPONDING
TO THE EMAIL ADDRESSES
(i) DOETRISTIN2@MAIL.COM,
(ii) LAWRENCEBISHOP13@YAHOO.COM,
AND
(iii) TRISTINJAMES6969@GMAIL.COM
THAT ARE STORED AT PREMISES
CONTROLLED BY DROPBOX, INC.,
LOCATED IN THE NORTHERN DISTRICT
OF CALIFORNIA.

Case No. _____

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, David C. Fallon, being first duly sworn, hereby depose and state as follows:

1. I have been employed as a Special Agent of the Federal Bureau of Investigation (FBI) since May 19, 1991, and I am assigned to the Albany Division, Albany, New York. My experience as an FBI Agent includes conducting hundreds of criminal investigations in the Northern District of New York. I have been a Special Agent of the FBI for over twenty-five years. I have conducted numerous investigations of computer-related crimes including crimes associated with the possession, distribution, and production of child pornography and child exploitation using the Internet. I am also a member of the FBI's Child Abduction Rapid Deployment Team with extensive specialized training related to conducting, leading, and managing investigations related to missing and abducted children. I also serve as the case agent for the Albany Division's Child Exploitation Task Force, which targets online child sexual predators and those individuals who trade child pornography. Prior to being employed as a

Special Agent, I was an attorney licensed to practice law in the State of Rhode Island.

2. I make this affidavit in support of an application for a search warrant for Dropbox accounts corresponding to or associated with the email addresses doetrustin2@mail.com, lawrencebishop13@yahoo.com, and tristinjames6969@gmail.com (the "Accounts"), which are stored at premises owned, maintained, controlled, or operated by Dropbox, Inc. ("Dropbox"), headquartered at 185 Berry Street, 4th Floor, San Francisco, CA 94107, hereinafter referred to as the "premises," and further described in Attachment A, attached hereto.

3. The information contained in this affidavit is based on my knowledge and on observations made by me during the course of this investigation, on information conveyed to me by other law enforcement officers, and on my examination and review of physical evidence obtained during the investigation.

4. Because this affidavit is being submitted for the limited purposes of securing a search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe establish a violation of federal law and that evidence of that crime is presently within the Accounts to be searched.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of 18 U.S.C. § 2252A, relating to material involving the sexual exploitation of minors.

a. 18 U.S.C. § 2252A(a)(2) prohibits knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

b. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing

any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer.

In my training and experience, people who possess, receive or distribute child pornography, particularly those doing so through the Internet, almost always have a connection to child pornography that has passed through interstate and foreign commerce.

DROPBOX, INC.

6. “Dropbox” refers to an online storage medium on the Internet accessed from a computer or electronic storage device. As an example, online storage mediums such as Dropbox make it possible for the user to have access to saved files without the requirement of storing said files on their own computer or other electronic storage device. Dropbox is an “offsite” storage medium for data that can be viewed at any time from any device capable of accessing the Internet. Users can store their files on Dropbox and avoid having the files appear on their computer. Anyone searching an individual’s computer that utilizes Dropbox would not be able to view these files if the user opted only to store them at Dropbox, the “offsite.” Based on my training and experience, I know that such “offsites” are often viewed as advantageous by collectors of child pornography in that they afford collectors an added level of anonymity and security.

7. Dropbox provides a variety of online services to the public, including online storage access. Dropbox allows subscribers to obtain accounts at the domain name

www.dropbox.com. Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other personal identifiers; alternative e-mail addresses; and, for paying subscribers, the means and source of payment (including a credit card or bank account, identified by a credit card or bank account number).

8. When the subscriber transfers a file to a Dropbox account, the file is (1) initiated at the user's computer, (2) transferred via the Internet to the Dropbox servers, and then can (3) automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. The process necessitates online storage of the file on Dropbox servers. If the subscriber does not delete the content, the files can remain on Dropbox servers indefinitely. Even if the subscriber deletes their account, the content may continue to be stored on the Dropbox servers for a certain period.

9. Online storage providers such as Dropbox, Inc., typically retain certain transactional information about the creation and use of each account on their systems. This information typically includes the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to

identify which computers or other devices were used to access the account.

10. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

BACKGROUND OF THE INVESTIGATION

11. Starting on July 7, 2016 and continuing to November 8, 2016, the New York State Police Internet Crimes Against Children Task Force (ICAC) received four CyberTipline Reports from Google, Inc., and Dropbox, Inc., with information indicating that an individual utilizing IP Address 2606:6000:e644:3c00:1d60:e57d:6d9e:e8b6 (IPv 6), among several others, was uploading sexually explicit images and videos of children to a Google+ Photo account with the email address tristinjames6969@gmail.com and to Dropbox accounts associated with the email accounts lawrencebishop13@yahoo.com and tristinjames6969@gmail.com.

12. Investigation by ICAC investigators and FBI Child Exploitation Task Force member John Montesano determined that IP Address 2606:6000:e644:3c00:1d60:e57d:6d9e:e8b6 was subscribed to by David Larose with service at 584 Central Avenue, Apt. 1, Albany, New York. Subsequent investigation by ICAC determined that Larose was the landlord of the address and did not live there himself.

13. Public-records database checks conducted by ICAC personnel revealed that a Conika J. Waldron lived in Apartment 1 at 584 Central Avenue. Further, these database checks revealed that a Michael GULLINESE was residing in Apt. 2 at the same address.

14. Further investigation regarding GULLINESE revealed that he was a registered sex offender having been federally convicted of possessing and receiving child pornography in 2009 in the Northern District of New York. He had been sentenced to 5 years in prison and a term of supervised release on the 2009 conviction. He was released from prison in 2014 and has been under the supervision of the United States Department of Probation and Parole since then. According to U.S. Probation Officer Ed Cardinal, GULLINESE does not participate in the U.S. Probation Office's computer monitoring program as he has repeatedly advised his assigned probation officers that he does not possess any devices capable of accessing the Internet.

15. On March 10, 2017, TFO Montesano applied for and received a search warrant from the City of Albany, Local Criminal Court, to search the residence and computers located at 584 Central Avenue, Apt. 1, Albany, NY for evidence related to the distribution of child pornography. Law enforcement executed the warrant on March 14, 2017.

16. When the warrant was executed, U.S. Probation Officers Stephanie Meyers and Jay Driscoll, along with your affiant, conducted a probation check on GULLINESE in Apt. 2 at the same address. Simultaneous to the execution of the warrant in Apt. 1, we interviewed GULLINESE for any information he may have regarding the distribution, receipt and possession of child pornography through Dropbox and/or Google.

17. During the interview, GULLINESE admitted that he used the Dropbox account associated with the email address tristinjames6969@gmail.com to store images and videos of child pornography that he obtained from other individuals that he communicated with over the Internet, particularly via Kik Messenger. GULLINESE admitted to purchasing a Cricket Wireless cellular telephone approximately 8 months earlier and hiding the Internet-capable

device from his probation officers. He further admitted that he created the tristinjames6969@gmail.com email account after purchasing the Cricket Wireless cellular telephone. GULLINESE advised that he had last accessed his Dropbox account on March 13, 2017. GULLINESE told PO Driscoll that the cell phone was under the mattress in his bedroom and gave consent for PO Driscoll to search his apartment for the phone and any other Internet-capable devices that he may have secreted there. The cell phone was found under GULLINESE's mattress by PO Driscoll.

18. Thereafter, GULLINESE provided written consent for your affiant to search the phone for evidence of GULLINESE's activities on Dropbox, Gmail and Kik, among other web- and cellular-based apps and sites. *See* Attachment C.¹ GULLINESE also provided your affiant with written consent to search the Dropbox account associated with email address tristinjames6969@gmail.com; to search his Kik Messenger account, tristinhotboi; and to assume his online identities in said Dropbox and Kik accounts as well as in his Gmail account, tristinjames6969@gmail.com.

19. On March 15, 2017, your affiant attempted to access the Dropbox, Gmail and Kik accounts that GULLINESE granted consent to search and assume. Upon logging in to the Dropbox account associated with the email address tristinjames6969@gmail.com, your affiant was advised that the account was disabled and therefore inaccessible. Upon attempting to log in to the Gmail account tristinjames6969@gmail.com, your affiant was advised via automatic

¹ Note that there appears to be a typo in the consent forms, in that "Tristin" appears to have been spelled "Tristan" throughout. I have determined that "Tristin"—at it appears throughout this affidavit and in the warrant itself—is the correct spelling.

notification that “Google doesn’t recognize the email address.” Your affiant was therefore unable to access the Gmail account.

20. Your affiant was able to access GULLINESE’s Kik account, tristinhotboi. There, your affiant observed that GULLINESE had been chatting with numerous individuals and exchanging sexually explicit images and videos of children through these chats. In some instances, the sexually explicit images and videos were transferred directly via Kik; in others, GULLINESE provided a link to a Dropbox account through which the images and video could be accessed. Based on my review, it appeared that these communications occurred into March 2017.

21. Because your affiant was unable to log onto the Dropbox and Gmail accounts, and because GULLINESE had granted your affiant written consent to search his phone, on March 16, 2017, your affiant conducted a search of GULLINESE’s cellular phone while it was in “airplane” mode and therefore unable to send or receive any radio or cellular signals. Your affiant observed the Dropbox application icon on the “desktop” of the phone. Upon accessing this application, your affiant found that the email address associated with the Dropbox account programmed into the application was not tristinjames6969@gmail.com, but rather doetrustin2@mail.com. Accordingly, your affiant assumes that GULLINESE was being untruthful when he provided the name of the email account associated with his Dropbox to your affiant and U.S. Probation.

22. While accessing the Dropbox account on the phone, your affiant observed several video files with file names indicative of child pornography. These included “boysexparty,” “13yo black boy,” and “14yo black boy.” Because these files are stored on Dropbox and not on

the cell phone itself, however, your affiant was unable to play or otherwise access them to determine their content.

23. Your affiant also accessed the Kik Messenger application found on GULLINESE's cellular phone and determined that the associated email address was lawrencebishop13@yahoo.com. This is the same email address listed in a CyberTip Report sent by Dropbox to the National Center for Missing and Exploited Children (NCMEC) indicating that an individual was uploading child pornography to said Dropbox account from an IP Address associated with 584 Central Avenue, Apt. 1, Albany, NY. Further, upon accessing the Yahoo email icon on GULLINESE's phone, your affiant observed that the Yahoo email account listed was lawrencebishop13@yahoo.com.

24. As discussed above, Dropbox is well known to me as a web site through which people view, possess receive and distribute child pornography. This is because Dropbox permits people to store images and videos on computer servers that are physically far away from their own computing devices.

25. In my experience, and based on prior investigations, I know that people interested in child pornography store digital files containing child pornography in Dropbox accounts, which are considered a more surreptitious – and therefore “safer” – way of accessing child pornography than receiving or sending it through a peer-to-peer network such as BitTorrent where law enforcement officers routinely operate undercover.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

26. Based on the information above, there is probable cause to conclude that Michael GULLINESE was using Dropbox accounts corresponding to the email addresses (i)

doetrustin2@mail.com, (ii) lawrencebishop13@yahoo.com, and/or (iii) tristinjames6969@gmail.com to possess child pornography.

27. Based on the information above, I believe there is probable cause to conclude that on the computer systems owned, maintained and/or operated by Dropbox, Inc., headquartered at 185 Berry Street, 4th Floor, San Francisco, CA 94107, there exists evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A. By this affidavit and application, I request that the Court issue a search warrant directed to Dropbox, Inc., allowing agents to search the locations described in Attachment A and seize the items described in Attachment B.


28. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox, Inc., to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

29. Based on the foregoing, I respectfully request that the Court issue the proposed search warrant.

30. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States (including a magistrate judge of such a court) . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

31. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.



David C. Fallon, Special Agent
Federal Bureau of Investigation

SUBSCRIBED AND SWORN to before me
this 31st day of March, 2017.



Hon. Daniel J. Stewart
United States Magistrate Judge

ATTACHMENT A

LOCATION TO BE SEARCHED

The property to be searched consists of any Dropbox account corresponding to or associated with the email addresses doetrustin2@mail.com, lawrencebishop13@yahoo.com and/or tristinjames6969@gmail.com that are stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., headquartered at 185 Berry Street, 4th Floor, San Francisco, CA 94107.

ATTACHMENT B

ITEMS TO BE SEIZED

I. Information to be disclosed by Dropbox, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Dropbox, Inc., including any messages, records, files, logs, or information that have been deleted but are still available to Dropbox, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Dropbox, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, and the date and time at which each file was sent;

b. All transactional information of all activity of the Dropbox, Inc. accounts, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting; and emails “invites” sent or received via Dropbox, and any contact lists.

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between Dropbox, Inc. and any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § § 2252A(a)(2)(A) (distribution and receipt of child pornography) and 2252A(a)(5)(B) (possession of child pornography)² including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Subscriber information, such as name, email address, zip code and other personal/biographical information;

(b) Account access information, master and sub account names, user profiles, friends lists, instant messages, grief reports, account creation information, associated IP information for each account use, screen shots of account activity, email transaction information;

(c) Information relating to transportation, distribution, receipt, and possession of image and movie files that contain of child pornography, as that term is defined in 18 U.S.C. § 2256;

² The term “child pornography” as used in this search warrant, is as defined in 18 U.S.C. § 2256(8).

- (d) Stored image and video files of any minor engaged in sexually explicit conduct as defined in Title 18, U.S.C. § 2256;
- (e) Any information pertinent to identifying any minor or minors portrayed in any image or video found within the accounts, including any correspondence or other communication with said minors;
- (f) Any record of an attempt to commit the listed offenses (18 U.S.C. § 2252A(a)(2)(A) and 2252A(a)(5)(B)) including any correspondence soliciting or otherwise discussing sexually explicit conduct by or with minors, including discussions of or solicitation for meeting with minors and/or for images or videos of minors;
- (g) Any images or videos of minors, such as child erotica, that evidence a sexual interest in children and/or an attempt to produce, receive, or possess child pornography;
- (h) The identity of the person(s) who created or used the user accounts listed in Attachment A;
- (i) The identity of any person(s) who communicated with the user accounts listed in Attachment A about matters relating to the enticement of a minor to engage in unlawful sexual activity, as defined in 18 U.S.C. § 2422(b), the receipt and distribution of child pornography, as defined in 18 U.S.C. § 2252A, and the possession of child pornography, as defined in 18 U.S.C. § 2252A.

III. Method of delivery

Items seized pursuant to this search warrant can be served by sending, on any digital media device, to the Special Agent designated on email address used to provide Dropbox with the Search Warrant at: Federal Bureau of Investigation, 200 McCarty Avenue, Albany, NY 12209.

ATTACHMENT C

CONSENT TO SEARCH COMPUTER/ ELECTRONIC EQUIPMENT

I, Michael Gullinrese, have been asked to give my consent to a search. I have also been informed of my right to refuse to consent to such a search.

I hereby authorize David Fallon, FBI and any other person(s) designated by [insert Agency/Department] to search:

(check as many as apply)

- ☐ The premises at street address _____, and any storage media or other computer/electronic equipment located therein, including internal hard disk drive(s), floppy diskettes, compact disks, scanners, printers, other computer/ electronic hardware or software and related manuals; any other electronic storage devices, including but not limited to, personal digital assistants, cellular telephones, and electronic pagers; and any other media or materials necessary to assist in accessing the stored electronic data.

- ☒ The following storage media or electronic devices:

Android ZTE cell phone (cell # 518-368-1257)
Description of computer, data storage device, cellular telephone, or other device (make, model and serial number, if available)

PSWC 88942001

I consent that search may be for any purpose, and that the search may include the examination of computer data and the use of forensic review

CONSENT TO SEARCH

Cloud-Based/Remote-Storage Accounts

Case Number: _____

I, Michael Gullinese, hereby voluntarily provide consent to officers of the Federal Bureau of Investigation to conduct a complete search of my following cloud-based/remote-storage accounts, which may include, but is not limited to, webmail, social media, online file storage, media storage, remote backups, and location services:

ACCOUNT PROVIDER	USERNAME/LOGIN ID	PASSWORD/PHRASE
Dropbox	tristanjames6969	alici969882001
kik	tristanhotboi	" "

I have authority to access and use the above accounts and all information found in them. I understand that law enforcement officers will change the passwords to these accounts so that I will no longer have access to these accounts. I authorize law enforcement officers to access the above accounts as necessary to seize items which they determine may be relevant to their investigation. I have been advised of my right to refuse consent. I give this consent freely and voluntarily.

I understand that I may contact SA David Fallon at the FBI by phone at 518-431-7345 or by email at _____ and may revoke my consent at any time.

3/14/17 Date Michael T Gullinese Signature

Witness: SA Dale RLL SA FBI

CONSENT TO SEARCH COMPUTER/ ELECTRONIC EQUIPMENT

I, Michael Gullinrese, have been asked to give my consent to a search. I have also been informed of my right to refuse to consent to such a search.

I hereby authorize David Fallon, FBI and any other person(s) designated by [insert Agency/Department] to search:

(check as many as apply)

- ☐ The premises at street address _____, and any storage media or other computer/electronic equipment located therein, including internal hard disk drive(s), floppy diskettes, compact disks, scanners, printers, other computer/ electronic hardware or software and related manuals; any other electronic storage devices, including but not limited to, personal digital assistants, cellular telephones, and electronic pagers; and any other media or materials necessary to assist in accessing the stored electronic data.
- ☒ The following storage media or electronic devices:

Android ZTE cell phone (cell # 518-368-1257)
Description of computer, data storage device, cellular telephone, or other device (make, model and serial number, if available)

PSWC 28942001

I consent that search may be for any purpose, and that the search may include the examination of computer data and the use of forensic review

techniques. I consent to the search occurring at any time, for any length of time, and at any location.

If any of the devices described above are protected with a password and/or encrypted, I consent to the use of my passwords and/or encryption keys to access the data. The password(s) and/or encryption keys are:

88942001

I certify that I have a right to access or use these devices and all information found in them. I understand that any contraband or evidence on these devices may be used against me in a court of law.

I relinquish any constitutional right to privacy in these electronic devices and any information stored on them. I authorize [insert Agency/Department] to make and keep a copy of any information stored on these devices. I understand that any such copy will not be my property and that I will have no privacy or possessory interest in the copy.

This written permission is given by me voluntarily. I have not been threatened, placed under duress, or promised anything in exchange for my consent. I have read this form, or it has been read to me, and I understand it. I understand the [English] language and have been able to communicate with the agents/officers.

I understand that I have the right to withdraw my consent to the [agency's] search of my original physical storage media or electronic devices. I understand that I may ask for a receipt for all things turned over.

Michael T Gullin
Signature

3/14/17 8:52 am
Date and time

Michael T Gullin
Name (printed)

Signature of Witnesses:

SA D. O. RIL SA FB
3-14-17 8:52 AM

CONSENT TO SEARCH

Cloud-Based/Remote-Storage Accounts

Case Number: _____

I, Michael Gullinase, hereby voluntarily provide consent to officers of the Federal Bureau of Investigation to conduct a complete search of my following cloud-based/remote-storage accounts, which may include, but is not limited to, webmail, social media, online file storage, media storage, remote backups, and location services:

ACCOUNT PROVIDER	USERNAME/LOGIN ID	PASSWORD/PHRASE
Dropbox	tristanjames6969	alici969882001
iCloud	tristanhotboi	" "

I have authority to access and use the above accounts and all information found in them. I understand that law enforcement officers will change the passwords to these accounts so that I will no longer have access to these accounts. I authorize law enforcement officers to access the above accounts as necessary to seize items which they determine may be relevant to their investigation. I have been advised of my right to refuse consent. I give this consent freely and voluntarily.

I understand that I may contact SA David Fallon at the FBI by phone at 518-431-7345 or by email at _____ and may revoke my consent at any time.

3/14/17 Date Michael T Gullinase Signature

Witness: SA Dale Full SA FBI

techniques. I consent to the search occurring at any time, for any length of time, and at any location.

If any of the devices described above are protected with a password and/or encrypted, I consent to the use of my passwords and/or encryption keys to access the data. The password(s) and/or encryption keys are:

88942001

I certify that I have a right to access or use these devices and all information found in them. I understand that any contraband or evidence on these devices may be used against me in a court of law.

I relinquish any constitutional right to privacy in these electronic devices and any information stored on them. I authorize [insert Agency/Department] to make and keep a copy of any information stored on these devices. I understand that any such copy will not be my property and that I will have no privacy or possessory interest in the copy.

This written permission is given by me voluntarily. I have not been threatened, placed under duress, or promised anything in exchange for my consent. I have read this form, or it has been read to me, and I understand it. I understand the [English] language and have been able to communicate with the agents/officers.

I understand that I have the right to withdraw my consent to the [agency's] search of my original physical storage media or electronic devices. I understand that I may ask for a receipt for all things turned over.

Michael T Gullinese
Signature

3/14/17 8:52 am
Date and time

Michael T Gullinese
Name (printed)

Signature of Witnesses:

SA D. O. RIL SA FB
3-14-17 8:52 AM

FD-1086
1-24-2012FEDERAL BUREAU OF INVESTIGATION
CONSENT TO ASSUME ONLINE IDENTITY AUTHORIZATION FORM

I, Michael Gullinese, hereby voluntarily authorize
SA David Fallon or other agents of the FBI to assume and use my
(or my child's) "online identity". I give this consent freely and voluntarily, without fear, threats, coercion, or
promises of any kind. I have been advised of my right to refuse to allow the FBI to assume my (or my child's)
online identity, and I hereby voluntarily waive this right. This online identity includes the following screen
name(s), aliases and/or nickname(s), and/or e-mail addresses, as well as the passwords associated with these
accounts:

ACCOUNT NAME

Kik Messenger - tristanhotboi
Drobox: tristanjames6969@gmail.com
Gmail: tristanjames6969@gmail.com

PASSWORD

alicia 69882001
alicia 69882001
alicia 69882001

This authorization provides my consent to:

- Monitor incoming and/or outgoing communications
- Use and/or disclose accessed information
- Send/receive/communicate

I understand and acknowledge that by signing the consent form, I relinquish all present and future claims to the
use of these accounts (or my child's). I understand that the FBI will change the password(s) to this
account so that I will no longer have access.

Signature: Michael T. GullineseName (printed): Michael T. GullineseDate: March 14, 2017Witness: D. J. SullivanName (printed): DAVID FALLONOfficial Title: SADate: 3-14-2017Witness: Edward CordinaName (printed): S.C.S. Probation OfficeOfficial Title: S.C.S. Probation OfficeDate: 3/14/17

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Dropbox, Inc., and my official title is _____. I am a custodian of records for Dropbox, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Dropbox, Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Dropbox, Inc.; and
- c. such records were made by Dropbox, Inc., as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature